

CYBERCRIME DALAM ABAD 21 : SUATU PERSPEKTIF MENURUT HUKUM INTERNASIONAL

Sinta Dewi

Dosen Fakultas Hukum, Universitas Padjadjaran Bandung.

Abstract

The development of information technology has encouraged the development of rapid Demian use of the Internet to conduct transactions in the world. Today virtually all parties have used the Internet both for individuals, businesses and government agencies. However, the global Internet usage has led certain parties to commit crimes in cyberspace or cybercrime. Because of human activities in the cyber world is limitless activities that have an international dimension, the transnational nature of crimes committed so that when viewed from the global rate of loss has exceeded the crimes committed due to drug sales. To deal with this problem it is necessary that takes into account protection through regulatory harmonization Globally and will be able implementad in national regulations. This research purpose are to analyze several legal issues such as how International Law Play an Important Role in Regulationd and urge international Cooperation to combat Cybercrime. This research used a normative juridical approach which focuses on secondary data, then used all the legal and juridical methods of historical comparison is obtained from the research literature is supported by primary data from field research. The specifications of research used is descriptive analytical and subsequent data collected were analyzed qualitatively. Based on the research and data analysis can be concluded that International Law has play an important role in regulating Cyberlaw and has promote international cooperation in combating Cybercrime and at the same time will encourage the harmonization of Cyberlaw Regulations.

Key words: Hukum Internasional, Cybercrime, Harmonization

Globalisasi telah menyatukan ekonomi dunia, sehingga batas-batas antar negara dalam berbagai praktik bisnis seakan-akan dianggap tidak berlaku lagi.¹ Sesuai dengan pendapat Sander yang menyatakan globalisasi sebagai suatu proses ketika negara-negara mulai menghilangkan hambatan-hambatan sehingga tercipta suatu dunia yang lebih terbuka dan tanpa batas.² Salah satu faktor pendorong globalisasi adalah teknologi informasi yang memungkinkan manusia untuk saling berhubungan tanpa dibatasi oleh batas-batas negara sehingga dunia seakan-akan menjadi datar.³ Menurut Alvin Toffler, dunia saat ini menuju gelombang keempat (*the present fourth wave of globalization*) yaitu globalisasi di segala bidang.⁴ Salah satu pilar globalisasi adalah penggunaan komunikasi yang

merupakan pilar utama hubungan internasional dengan menggunakan kemajuan teknologi informasi. Dalam perkembangannya, kemajuan teknologi informasi telah mendorong negara-negara untuk meliberalisasi sektor komunikasi sehingga mendorong kompetisi dan globalisasi komunikasi dan pada akhirnya telah menstimulasi kemajuan ekonomi.⁵

Dunia saat ini sedang berada dalam abad informasi yang keberadaan suatu informasi mempunyai peranan yang sangat penting di dalam kehidupan manusia. Melalui kemajuan informasi, komunikasi, dan teknologi (*Information Communication Technology/ICT*) merupakan salah satu faktor utama yang mendorong perkembangan dan pertumbuhan ekonomi dunia.⁶ Saat ini, informasi

1. Hendra Halwani, 2002, *Ekonomi Internasional & Globalisasi Ekonomi*, Jakarta, Ghalia, hlm. i

2. Seperti yang dikutip dalam Nanang Pamuji Mugasejati dan Ucu Martanto (ed), 2006, *Kritik Globalisasi & Neoliberalisme*, Yogyakarta, hlm. 2.

3. Thomas L. Friedman, 2006, *The World is Flat*, Penguin Books, London, hlm. 10.

4. Seperti yang dikutip di dalam Sunaryati Hartono, 2006, *Bhineka Tunggal Ika Sebagai Asas Hukum bagi Pembangunan Hukum Nasional*, Penerbit PT Citra Aditya Bakti, Jakarta, hal 41. Menurut Thomas L. Friedman, *op.cit*, hlm 11. Melalui globalisasi yang menggunakan kemajuan teknologi informasi telah menyebabkan jarak antar negara menjadi sangat dekat sehingga dunia seakan-akan berbentuk mendatar.

5. John Baylis & Steve Smith, 2001, *The Globalization of World Politics, An Introduction to International Relations*, New York, Oxford University Press, hlm. 540-541.

6. Kofi A. Anan, 2004, *UNCTAD E-commerce and Development Report*, hlm. 4.

merupakan komoditi yang mempunyai nilai ekonomi tinggi karena tidak semua pihak mampu untuk memproses dari suatu data yang mentah menjadi suatu informasi yang sesuai dengan kebutuhannya⁷. Salah satu bidang ilmu pengetahuan dan teknologi yang diandalkan di dunia internasional dan nasional adalah teknologi informasi yang diharapkan dapat menjadi salah satu tulang punggung untuk mendorong kemajuan ekonomi seperti yang disampaikan oleh *Francis Bacon* bahwa siapa yang menguasai informasi maka pihak tersebut memiliki kekuatan termasuk kekuatan ekonomi.⁸

Perkembangan teknologi informasi kemudian bertambah pesat didorong oleh terjadinya konvergensi antara teknologi informasi⁹, telekomunikasi, dan penyiaran sehingga memungkinkan orang untuk mengumpulkan, menyimpan, memproses, dan menyebarkan suatu informasi. Interaksi antara ketiga jenis teknologi di atas, telah mendorong manusia untuk memanfaatkan kemajuan teknologi tersebut dengan memadukan metode-metode telekomunikasi suara, data, dan tulisan serta gerak secara sekaligus yang dikenal dengan ISDN (*Integrated Services Digital Network*).¹⁰ Sebagaimana teknologi lainnya, selain memiliki kelebihan berupa kemudahan dan dapat memberikan manfaat luas yang meningkatkan kualitas kehidupan manusia, maka layanan perbankan elektronik juga memiliki banyak kelemahan yang patut diwaspadai dan diantisipasi, salah satunya adalah kejahatan melalui dunia internet atau disebut dengan *cybercrime*.¹¹

Pada abad 21 secara nasional jaringan *broadband* merupakan infrastruktur yang sangat penting sebagaimana halnya dengan transportasi, sumber daya energi dan air.¹² Jaringan interkoneksi dengan menggunakan internet secara global telah menciptakan suatu peluang ekonomi yang

sebelumnya belum pernah terjadi. Pertumbuhan pengguna internet telah menunjukkan perkembangan yang sangat pesat menurut data statistik yang dikeluarkan pada tahun 2010, internet *world statistics*¹³ pengguna internet secara global dari tahun 2000-2010 naik 380 % dan Asia merupakan kawasan pengguna internet terbesar yaitu 825,1 juta, Eropa sebesar 75,1 juta diikuti oleh Amerika Utara sebesar 266,2 juta, Amerika Latin sebesar 204,7 juta, Afrika sebesar 110,9 juta, negara-negara Timur tengah sebesar 63,2 juta dan wilayah Oceania dan Australia sebesar 21,3 juta pengguna.

Melihat kenaikan pengguna internet sebagai media dalam *cyberspace* maka *cyberspace* sekarang telah menjadi salah satu wilayah seperti halnya wilayah daratan, laut, udara, ruang udara dan kelima *cyberspace*.¹⁴ Potensi dan manfaat yang besar tersebut di atas, diikuti oleh tindakan-tindakan merugikan orang dan yang paling menonjol adalah kejahatan yang dilakukan secara *online* yaitu *cybercrime*. Tingkat kenaikan *cybercrime* yang sangat mengkhawatirkan telah mempengaruhi tingkat kepercayaan para pengguna atas *e-commerce* juga bagi pemerintah maupun pihak swasta dalam menjalankan kegiatan sehari-hari disamping itu serangan *cybercrime* juga telah mengganggu kepentingan publik dengan mengganggu jaringan infrastruktur publik seperti telepon, listrik, keuangan, pelayanan publik¹⁵.

Secara nasional maupun internasional, negara-negara berusaha mengamankan dengan memberikan perlindungan bagi masyarakat¹⁶ dengan membuat pengaturan dan dari segi teknologi berusaha mencari sistem baru untuk mengamankan jaringan informasi mereka.

Tingkat kejahatan dalam *cyberspace* atau *cybercrime* telah menunjukkan kenaikan sangat tinggi secara global, regional maupun nasional sehingga

7. Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, PT Raja Grafindo Perkasa, Jakarta, hlm. 3. Lihat juga M. Arsyad Sanusi, 2004, *Teknologi Informasi & Hukum E-commerce*, PT Dian Ariesta, Jakarta, hal. 9. Menurut Branscomb, 1983, *Information is the Lifeblood that sustain political, social and business decision*, dalam Anne W. Branscomb, *Global Governance of Global Networks: A survey of Transborder Data Flows in Transition*, *Vanderbilt Law Review*, Vol. 36, hal. 985.

8. Ian J. Lloyd, 2000, *Information Technology Law*, Butterworth, London, hal. xxxviii.

9. Maureen S. Dorney, 1998, "Privacy and the Internet", *Hasting Communications and Entertainment Law Journal*, Vol. 19, hlm. 636.

10. Dedi Supriadi, 1995, *Era Baru Bisnis Telekomunikasi*, Bandung, PT Rosda Jayaputra, 1995, hlm. 7.

11. Mohamad Salahuddin dalam <http://www.idstir.or.id/index.php/news/2010/01/21/81/mewaspadai-kejahatan-layanan-perbankan-elektronik-himbauan-kepada-masyarakat-dan-keterangan-pers.html>, diakses tanggal 10 September, 2010.

12. Hamadoun Toure, <http://www.pwc.com/gx/en/communications/review/perspective/hamadoun-toure.html>, diakses tanggal 31 Oktober, 2010.

13. <http://www.internetworldstats.com/stats.htm>, diakses tanggal 26 oktober, 2010.

14. Stein Schjolberg, 2010, *A Cyberspace Treaty- A United Nations Convention or Protocol on Cybersecurity and Cybercrime*, Background Paper dalam *The Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, Maret, hlm. 1-2.

15. Abraham D. Sofaer and Seymour E. Goodman, 2001, *Cyber Crime and Security : The Transnational Dimension* dalam *Transnational Dimension of Cyber Crime and Terrorism*, Abraham D. Sofaer and Seymour E. Goodman (ed), USA, Hoover Institution Press Publications, hlm. 1-2.

16. ITU Toolkit, dalam <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>, halaman diakses tanggal 25 Oktober, 2010.

tingkat kejahatan yang dilakukan meningkat tajam. Menurut Sekretaris Jenderal ITU Hamadoun Toure, bahwa tantangan yang harus dihadapi oleh negara-negara adalah keamanan dalam *cyberspace* mengingat hampir semua orang mendapatkan akses internet. Kerugian secara global dari *Cybercrime* pertahun sudah mencapai 100 milyar dolar Amerika.¹⁷

Selanjutnya menurut informasi yang dikeluarkan SOCA (*Serious and Organized Crime Agency*) Inggris saat ini *cybercrime* berkaitan erat dengan jenis kejahatan lainnya yaitu jual beli obat bius, perjudian, terorisme dan juga berkaitan erat dengan organisasi kejahatan lainnya seperti dengan Mafia, Yakuza, Kartel Kolumbia, Mafia Rusia dan Malaysia dan jenis kejahatan nya berubah sejak 2006 yang awalnya merupakan kejahatan *tradisional* menjadi jenis kejahatan dengan motif ekonomi.¹⁸ Selanjutnya, para pelaku kejahatan ini memperluas jaringan secara global dan kini organisasi-organisasi kejahatan melakukan operasi kejahatannya melalui *cyberspace*²⁰ dengan adanya kerjasama antara organisasi dan pelaku kejahatan di *cyberspace* telah menyebabkan *digital world* menjadi lebih tidak aman.²¹ Menurut Wolfe & Wade sedikitnya 10 juta komputer seluruh dunia yang dirusak oleh hacker juga telah merusak jaringan komputer milik Pentagon, Gedung Putih, NATO. Pihak swasta juga tidak luput dari serangan *hacker* yang telah mencuri kode rahasia Microsoft dan melakukan *carding* terhadap bank-bank di Amerika Serikat.²²

Kesulitan lainnya yaitu karena sifat kejahatannya yang transnasional karena semua pesan data dan informasi melalui *packets* akan dikirimkan ke seluruh

dunia sehingga *cybercrime* merupakan salah satu jenis kejahatan yang sangat luas cakupannya (transnasional)²³ maka sangat sulit untuk melakukan penegakkan hukum karena memerlukan kerjasama diantara negara-negara yang memerlukan waktu lama karena prosesnya begitu rumit sehingga akhirnya pelaku terlepas dari jeratan hukum disebabkan setiap negara mengatur secara berbeda.²⁴ Kondisi ini dianggap merupakan salah satu kelemahan dalam proses penegakkan hukum walaupun selama ini negara-negara secara bilateral sering melakukan kerjasama bilateral melalui ekstradisi akan tetapi diperlukan kerjasama internasional yang lebih intensif melalui suatu perjanjian internasional. Sehingga peran Hukum Internasional sangat diperlukan untuk mengatur *cybercrime* sehingga akan tercipta suatu harmonisasi hukum sehingga para pelaku kejahatan dapat ditangkap dan diadili.

Melihat kondisi yang berkembang begara-negara baik secara nasional melalui pengaturan dan internasional melakukan upaya untuk mengamankan aktivitas melalui *cyberspace* melalui langkah-langkah teknis maupun non teknis dan salah satunya melalui harmonisasi.

Metode penelitian yang digunakan dalam penelitian ini adalah deskriptif analitis yaitu memaparkan data sebagaimana adanya untuk kemudian dilakukan analisis terhadap data tersebut berdasarkan kaidah-kaidah yang relevan.²⁵ Penelitian ini akan mengkaji dan menganalisis tentang Perkembangan *Cybercrime* Pada Abad ke 21 dan Bagaimana Peran Hukum Internasional dalam mengatur *Cybercrime* sebagai upaya untuk

17. I believe that cyber security is one of the greatest challenges that humanity is facing. Given the importance of our access to information and communication technology, the safety of our networks becomes a high priority. Cyber crime is on the rise and it's placing a huge burden on governments and the industry alike. In fact, the CEO for McAfee recently estimated that cyber crime is worth over \$100 billion annually, which is more than the total value of the global illegal trade in drugs. This emphasises how important cyber security is becoming.

I hope I'm wrong, but a next world war may well start on the Net, in cyberspace. Cyber war is not occurring right now, but some nation states are preparing themselves for it, and that's unfortunate. Cyber threats can reach parts of a nation that physical threats cannot. Attacks on critical infrastructure can stall a country's progress and quickly cause civil unrest. Cyberspace is driven by innovation and, unfortunately, the concept of a super power no longer exists in the way it did before: every individual on the planet can be a potential super power and can make an attack that can be lethal. Cyber threats have to be taken very seriously and that's why we urgently need to put in place a platform for global cooperation and coordination.

18. Izwan Ismail, 2008, Understanding Cyber Criminal, New Straits Times, 18 Februari, hlm. 5.

19. Nir Kshetri, 2010, *The Global Cybercrime Industry*, Springer Heidelberg Dordrecht London, New York, hlm. 1-3.

20. Ibid. hlm. 4

21. Seperti yang dikutip dalam Nir Kshetri, *Op. Cit.* hlm. 2.

22. Lihat Abraham D. Sofaer and Seymour E. Goodman, *Cyber Crime and Security : The Transnational Dimension dalam Transnational Dimension of Cyber Crime and Terrorism*, *Op.Cit.* hlm. 12.

23. Seperti yang dikutip dalam Susan W.Brenner and Marc D. Goodman, 2002, *Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice*, Paper, 2002, hal. 4. Salah satu contoh adalah penangkapan salah satu hacker Julio Cesar Ardita asal Argentina yang telah memasuki jaringan komputer Departemen Pertahanan Amerika Serikat akan tetapi Argentina menolak untuk melakukan ekstradisi karena menurut Pemerintah Argentina *Cybercrime* belum termasuk kejahatan yang masuk ke dalam perjanjian ekstradisi seperti yang dikutip dalam Lihat Abraham D. Sofaer and Seymour E. Goodman, *Cyber Crime and Security : The Transnational Dimension dalam Transnational Dimension of Cyber Crime and Terrorism*, *Op.Cit.* hlm. 17.

24. Soeyono Soekanto, 1982, *Pengantar Penelitian Hukum Edisi Kedua*, Jakarta, UI Press, 1982, hlm. 50.

melakukan harmonisasi hukum diantara negara-negara.

Metode pendekatan yang dipergunakan dalam penelitian ini adalah pendekatan *Juridis Normatif*²⁵, yaitu suatu metode pendekatan yang menekankan pada ilmu hukum disamping juga menelaah kaidah-kaidah hukum yang berlaku di masyarakat.²⁶

Spesifikasi penelitian yang digunakan adalah *deskriptif analitis*²⁷ yaitu untuk mendapatkan gambaran secara menyeluruh tentang Cybercrime serta menganalisis bagaimana peranan Hukum Internasional dalam mengatur Cybercrime.

Menurut Mochtar Kusumaatmadja Hukum Internasional merupakan keseluruhan kaidah dan asas hukum yang mengatur hubungan atau persoalan yang melintasi batas negara²⁸, selanjutnya Mochtar Kusumaatmadja menambahkan bahwa hukum internasional memiliki fungsi untuk menertibkan, mengatur dan memelihara hubungan internasional sehingga hukum internasional sangat dibutuhkan untuk menjamin kepastian hukum.²⁹ Salah satu bidang yang sangat memerlukan pengaturan Hukum Internasional adalah Cybercrime karena aktivitas pelaku telah meluas sehingga telah menimbulkan *global problem*³⁰ sehingga dalam hal ini sangat diperlukan peranan hukum internasional yang lebih besar.

Kegiatan cyber merupakan kegiatan yang memiliki dimensi global ditambah dengan kemajuan teknologi informasi yang sangat pesat sehingga sangat sulit bagi para pakar hukum untuk memberikan suatu definisi yang tegas mengenai jenis kejahatan ini. Hingga saat ini belum ada definisi yang dapat diterima oleh semua pihak hal tersebut disebabkan belum adanya kesepakatan tentang ruang lingkup kejahatan yang dilakukan dalam cyberspace. Menurut ITU³¹; *one common definitions describes cybercrime as any activity in which*

computers or networks are tools, a target or a place of criminal activity.

Selanjutnya Kshetri berpendapat bahwa *cybercrime is defined as a criminal activity in which computer or computer network are the principal means of committing an offence or violating laws, rules, or regulation.*³² Selanjutnya menurut Donn Parker secara umum harus dibedakan antara *computer crime* yaitu jenis kejahatan yang menggunakan komputer sebagai alat sedangkan *cybercrime* adalah jenis kejahatan dimana pelaku menggunakan *cyberspace* sebagai alat untuk melakukan kejahatannya.³³ Selanjutnya Roger LeRoy Miller menyatakan bahwa:³⁴ *A cyber crime is a crime that occurs in the virtual community of the internet.*

Cybercrime merupakan jenis kejahatan yang dilakukan oleh manusia yang melakukan aktifitas melalui internet. Departemen Hukum Amerika Serikat memberikan pengertian *Computer crime* sebagai *any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution* sedangkan Masyarakat Ekonomi Eropa memberikan definisi sebagai *any illegal act, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data.*³⁵ Jadi dapat disimpulkan secara umum bahwa kejahatan di bidang Cyber yaitu melakukan kejahatan-kejahatan dengan menggunakan komputer dan internet.

Konvensi Cybercrime, 2001 tidak berusaha membuat definisi hanya menggolongkan cybercrime kedalam 4 kategori yaitu : (1) *offences against the confidentiality, integrity and availability of computer data and systems*; (2) *computer related offences*; (3) *content-related offences*; (4) *offences related to infringement of copyright and related rights.*

Menanggulangi tingkat kejahatan yang sangat tinggi tersebut, maka negara-negara di dunia berkeinginan untuk membentuk harmonisasi hukum

25. Penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder dapat dinamakan penelitian hukum normative atau penelitian hukum kepustakaan yang mencakup : 1) Penelitian terhadap asas-asas hukum, 2) Penelitian terhadap taraf sinkronisasi vertikal dan horisantal, 3) Perbandingan hukum dan 4) Sejarah Hukum, Lihat Soeryono Soekanto, 1998 *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Jakarta, CV Rajawali, hlm. 15.

26. Roni Hanitjo Soemitro, 2001, *Metodologi Penelitian Hukum dan Jurimetri*, Jakarta, Ghalia Indonesia, hlm. 13.

27. *Ibid*, hlm. 11.

28. Mochtar Kusumaatmadja, Ety R. Agoes, 2003, *Pengantar Hukum Internasional*, Bandung, PT. Alumnus, hlm 1.

29. *Ibid*, hlm. 13.

30. Jonathan Clough, 2010, *Principles of Cybercrime*, Cambridge University Press, UK, hlm. 21.

31. Laporan ITU, Understanding Cybercrime for Developing Countries, 2009, dalam <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>, diakses tanggal 24 Oktober, 2010.

32. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>, diakses tanggal 24 oktober, 2010.

33. Seperti yang dikutip dalam Steven Furnell, 2002, *Cybercrime Vandalizing the Information Society*, Great Britain, Pearson Education Limited, hal 21.

34. Roger LeRoy Miller and Gaylord A. Jentz, 2001, *Law for E-Commerce*, West Thomas Learning, USA, hlm. 99.

35. Seperti yang dikutip dalam Petrus Reinhard Golose, 2006, *Perkembangan Cybercrime dan Usaha Penanganannya di Indonesia* oleh Polri, Buletin Hukum dan Kebanksentralan, Volume 4 Nomor 2, Agustus, hlm. 7.

baik secara substantif, prosedural sehingga dapat mengejar para pelaku dimanapun mereka berada karena jenis kejahatan ini merupakan jenis kejahatan transnasional yang sangat merugikan para pengguna internet.³⁶

Harmonisasi hukum merupakan suatu keharusan di dalam dunia yang global karena negara-negara dituntut untuk menyelaraskan prinsip-prinsip yang sama agar terjadi suatu keharmonisan. Harmonisasi hukum untuk pertama kalinya dikenal dalam hukum perdagangan internasional yang dilakukan oleh beberapa organisasi internasional seperti UNIDROIT dan UNCITRAL untuk menjembatani segala perbedaan pengaturan akibat dari perbedaan sistem hukum yang berlaku diantara negara-negara kemudian diikuti oleh bidang hukum lainnya.

Di Indonesia harmonisasi hukum telah diatur dalam Keputusan Presiden Nomor 188 Tahun 1998, yang isinya menyatakan pentingnya harmonisasi sebagai usaha untuk memantapkan suatu konsepsi yang akan dituangkan dalam RUU maka wajib melakukan harmonisasi.³⁷

Sejak berkembang pada awal tahun 1990 hingga sekarang, *cyberspace* telah membawa pengaruh yang sangat besar bagi umat manusia baik dari segi ekonomi, pemerintahan, politik, hukum bahkan budaya telah membawa perubahan yang sangat fenomenal bahkan menurut Stein Schjolberg *cyberspace* sudah merupakan wilayah yang kelima setelah wilayah daratan, lautan, udara dan ruang angkasa.³⁸ Akan tetapi pengaruhnya *cyberspace* tidak selamanya positif karena banyak digunakan untuk melakukan tindak *criminal* atau *cybercrime* yang sangat tinggi yang telah merugikan secara global. Hukum Internasional umum maupun regional telah memegang peran yang sangat aktif dalam menanggulangi meningkatnya *cybercrime* baik melalui kerjasama yang bersifat internasional maupun regional dan telah menyusun Konvensi maupun rekomendasi-rekomendasi seperti yang telah dilakukan baik oleh PBB maupun oleh organisasi internasional lainnya seperti ITU (*International Telecommunications Union*), OECD untuk menyelesaikan masalah ini secara global.

Mengingat aktivitas yang dilakukan dalam

cyberspace adalah transnasional termasuk kejahatan yang dilakukannya sehingga memiliki dimensi internasional sehingga penyelesaiannya memerlukan pendekatan internasional dan kerjasama internasional yang erat baik dari segi pengaturannya, pelaksanaannya dan penegakkan hukumnya sehingga akan menjamin adanya kepastian hukum sehingga pelaku tidak bisa lagi menikmati zona aman (*safe haven*) karena semua negara mengatur dan menerapkan *cyberlaw* secara konsisten.

Perserikatan Bangsa Bangsa (PBB)

Sebagai suatu organisasi dunia yang sangat penting, PBB telah berperan aktif dalam mengatur *Cybercrime* dengan mengeluarkan sejumlah Resolusi Majelis Umum PBB diantaranya adalah Resolusi 55/63 Tahun 2000 dan Resolusi 56/121 Tahun 2001 tentang *Combating the Criminal Misuse of Information Technologies* yaitu mendorong agar negara-negara untuk menerapkan hukum untuk mengatur penyalahgunaan teknologi informasi dengan demikian negara-negara tidak dijadikan tempat pelarian atau zona aman (*safe haven*) bagi pelaku kejahatan. Kemudian Resolusi 57/239, 2002 tentang *Creation of a Global Culture of Cybersecurity* dengan tujuan mendorong semua negara anggota PBB untuk bekerjasama untuk menjamin keamanan *Cyberspace* yang merupakan salah satu mekanisme negara-negara melakukan kerjasama sehingga selain menjamin keamanan juga negara-negara dihimbau untuk membangun suatu budaya dan etiket melakukan aktivitasnya di *Cyberspace* secara aman dan tidak merugikan pihak lain.³⁹ Selain itu Majelis Umum juga telah mengeluarkan resolusi no 58/199, 2003 tentang *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*. Resolusi ini lebih menitik beratkan pada urgensi negara anggota PBB untuk melindungi infrastruktur teknologi informasi sebagai salah satu sarana utama *Cyberspace*. Sebagai salah satu instrumen hukum internasional yang bersifat rekomendasi atau *soft law* maka resolusi hanya merupakan suatu anjuran saja akan tetapi secara

36. Stein Schjolberg & Amanda M. Hubbard, 2005, *Harmonizing National Legal Approaches on Cybercrime*, Paper dalam ITU WSIS Meeting on Cybersecurity, Jenewa, hlm. 1-5.

37. Kusnu Goesniadhie, 2006, *Harmonisasi Hukum dalam Perspektif Perundang-Undangan*, Surabaya, PT. Temprina Media Grafika, hlm. 69.

38. Stein Schjolberg, 2010, Paper dalam Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Brazil, hlm. 1.

39. <http://www.oecd.org/dataoecd/53/60/37019786.pdf>, diakses tanggal 10 Desember, 2010, hlm. 1.

moral telah mendorong masyarakat internasional untuk melindungi *cyberspace* walaupun hanya bersifat rekomendasi akan tetapi resolusi-resolusi tersebut di atas telah mengilhami organisasi internasional lainnya untuk juga membahas dan mengatur *Cybercrime*.

International Telecommunication Union (ITU)

ITU sebagai salah satu organisasi di bawah PBB yang membidangi masalah telekomunikasi juga telah mengadakan beberapa pertemuan internasional yang membahas *Cybercrime*, salah satunya dalam World Summit Information Society di Jenewa, 2002 dan di Tunisia pada tahun 2005. Kedua pertemuan internasional ini secara khusus membahas tentang kerjasama internasional tentang pemanfaatan teknologi informasi sebagai faktor yang sangat penting untuk mendorong perekonomian dan juga bekerjasama untuk menjamin keamanan *Cyberspace* dari pihak-pihak yang tidak bertanggung jawab. Disamping itu ITU menyusun *ITU Toolkit for Cybercrime Legislation*⁴⁰ untuk membantu negara-negara dalam menyusun perundangan tentang *Cybercrime*.

Aktivitas kedua organisasi dunia ini telah menunjukkan peran aktif dunia internasional dan hukum internasional dalam mengantisipasi dan memerangi *Cybercrime* walaupun hanya bersifat suatu rekomendasi akan tetapi telah mendorong organisasi lainnya terutama organisasi regional untuk menghadapi meningkatnya *Cybercrime* baik melalui Perjanjian internasional maupun rekomendasi-rekomendasi.

APEC (Asia Pasific Economic Cooperation)

Pada Tahun 2003, APEC menyusun suatu program yaitu *Capacity Building Project on Cybercrime*, program ini secara khusus mendorong negara-negara APEC untuk menyusun perundangan khususnya tentang *Cybercrime* termasuk memberikan pelatihan kepada pihak-pihak terkait dalam melakukan penyelidikan dan proses investigasi *Cybercrime*. Pada tahun 2005, APEC juga mengadakan Pertemuan Tingkat Menteri Telekomunikasi dan Informasi dan telah mengeluarkan Deklarasi yang isinya antara lain : (1) mendorong negara-negara anggota untuk mengatur secara lebih ketat *Cybercrime* dengan mengacu pada

Konvensi *Cybercrime*, 2001, (2) merekomendasi negara-negara untuk membuat undang-undang nasional yang secara komprehensif akan mengatur tentang *Cybersecurity* dan *Cyberlaw* yang konsisten dengan pengaturan hk internasional seperti Resolusi Majelis Umum No 55/63 Tahun 2000 dan dengan Konvensi *Cybercrime*. Akan tetapi dengan besarnya perbedaan-perbedaan diantara negara APEC maka perkembangan kearah harmonisasi hukum dalam pengaturan *Cybrcrime* masih belum memuaskan semua pihak karena masing-masing negara mengatur *cybercrime* secara berbeda.

Council of Europe

Council of Europe merupakan salah satu organisasi internasional yang bersifat telah berhasil menyusun suatu Konvensi yaitu *Convention on Cybercrime* yang ditandatangani di Budapest (Hungaria) tahun 2001 merupakan inisiatif internasional pertama yang mengatur tentang *cybercrime* yang ditandatangani di Budapest (Hungaria) tahun 2001. Konvensi ini telah dipersiapkan oleh *The Council of Europe* yang sejak tahun 1997 merancang *Proposal for a Convention Cybercrime*. Setelah melalui beberapa kali pembahasan, naskah *Convention on Cybercrime* disetujui dan ditandatangani oleh 38 negara (34 negara anggota Dewan Eropa dan 4 negara bukan anggota Dewan Eropa) di Budapest pada tanggal 23 November 2001. Sampai dengan bulan Oktober 2004 konvensi tersebut sudah ditandatangani 32 negara dan diratifikasi atau diakses oleh 8 negara anggota Dewan Eropa yaitu Albania, Croasia, Estonia, Hungaria, Lithuania, Macedonia, Romania, dan Slovenia.⁴¹

Masing-masing negara yang menandatangani dan meratifikasi sepakat untuk mengimplementasikan konvensi tersebut pada hukum pidana di masing-masing negara. Konvensi tersebut dijadikan standar minimum (*Standard Minimum Rules*) dalam penyusunan hukum pidana yang mengatur kejahatan yang berhubungan dengan komputer. Hal ini sesuai dengan tujuan utama konvensi tersebut sebagaimana tertuang dalam angka 16 penjelasan konvensi sebagai berikut.

The Convention aims principally at (1) harmonizing the domestic criminal substantive law elements of offences and connected provisions in the

40. <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>, diakses tanggal 10 Desember, 2010

41. <http://www.conventions.coe.int/treaty/commun/cherchesig.html>, diakses tanggal 25 Oktober, 2010.

area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computersystem or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation.⁴²

Konvensi diarahkan terutama dalam upaya (1) harmonisasi di unsur-unsur hukum yang mengatur pelanggaran dalam hukum pidana materil nasional dalam hubungannya dengan ketentuan *cybercrime*, (2) melengkapi hukum pidana formal nasional yang penting bagi proses penyelidikan, penyidikan, dan penuntutan terhadap pelanggar yang menggunakan atau ditujukan pada sistem komputer beserta alat-alat bukti yang berkaitan dengan kejahatan tersebut, dan (3) pengaturan terhadap kerjasama internasional agar lebih efektif dan cepat.

Konvensi terdiri dari empat (4) Bab⁴³ yaitu:

1. Bagian I (pertama) mengenai terminologi yang digunakan, terdiri atas 1 (satu) pasal yang berisi definisi-definisi tentang *computer system*, *service provider*, dan *traffic data* (Pasal 1 Konvensi).
2. Bagian II (kedua) mengenai langkah-langkah yang harus diambil pada tingkat nasional yang terdiri atas 21 (dua puluh satu) pasal, dan terbagi menjadi 3 (tiga) seksi, yakni (1) mengenai substansi hukum tindak pidana yang diatur (2) mengenai prosedur hukumnya dan (3) mengenai yurisdiksi (Pasal 2 sampai dengan Pasal 22 Konvensi).
3. Bagian III (ketiga) mengenai kerjasama internasional terkait dengan pelaksanaan ketentuan yang diatur dalam konvensi meliputi prinsip-prinsip ekstradisi, prinsip-prinsip umum yang berkaitan dengan bantuan timbal balik, pelaksanaan prosedur tentang permohonan bantuan timbal balik yang terdiri dari 13 (tiga belas) pasal dan terbagi menjadi 2 (dua) seksi, yakni (1) mengenai prinsip-prinsip umum dan (2) prinsip-prinsip khusus (Pasal 23 sampai dengan Pasal 35 Konvensi).
4. Bagian IV (keempat) yang merupakan bab terakhir yang mengatur tentang ketentuan-ketentuan standar mengenai hal-hal yang berkaitan dengan daya berlakunya konvensi dan

negara-negara peserta konvensi yang terdiri dari 13 (tiga belas) pasal.

Dari empat bab Konvensi tersebut, maka dimungkinkan untuk diadakan harmonisasi dalam hal legislasi yang terdiri dari empat (4) jenis pengaturan yaitu: 1) ketentuan hk pidana yang mengatur *cybercrime*; 2) proses; 3) program bantuan hukum; 4) perlindungan atas hak-hak pribadi.

Simpulan

Melihat peningkatan *Cybercrime* yang sangat besar maka masyarakat internasional harus melakukan kerjasama dan peran hukum internasional sangat penting untuk mengatur *Cybercrime* sehingga para pelaku kejahatan *Cyber* tidak akan menikmati zona aman (*safe Heaven*) di negara-negara yang belum mengatur masalah *Cybercrime* sehingga perlunya mengatur secara bersama tentang *Cybercrime*. Hingga saat ini Hukum internasional telah berperan untuk mengatur *Cybercrime* dan salah satunya melalui Konvensi *Cybercrime*.

Konvensi diarahkan terutama dalam upaya (1) harmonisasi di unsur-unsur hukum yang mengatur pelanggaran dalam hukum pidana materil nasional dalam hubungannya dengan ketentuan *cybercrime*, (2) melengkapi hukum pidana formal nasional yang penting bagi proses penyelidikan, penyidikan, dan penuntutan terhadap pelanggar yang menggunakan atau ditujukan pada sistem komputer beserta alat-alat bukti yang berkaitan dengan kejahatan tersebut, dan (3) pengaturan terhadap kerjasama internasional agar lebih efektif dan cepat.

DAFTAR PUSTAKA

- D. Sofaer Abraham and Seymour E. Goodman, 2001, *Cyber Crime and Security: The Transnational Dimension* dalam *Transnational Dimension of Cyber Crime and Terrorism*, Abraham D. Sofaer and Seymour E. Goodman (ed), USA: Hoover Institution Press Publications.
- Supriadi Dedi, 1995, *Era Baru Bisnis Telekomunikasi*, Bandung: PT Rosda Jayaputra.
- Makarim Edmon, 2003, *Kompilasi Hukum Telematika*, Jakarta: PT Raja Grafindo Perkasa.
- Halwani Hendra, 2002, *Ekonomi Internasional & Globalisasi Ekonomi*, Jakarta: P.T. Ghalia.

42. Stein Schjolberg & Amanda M. Hubbard, 2005, *Harmonizing National legal Approaches on Cybercrime*, Paper dalam WSIS Thematic Meeting on Cybersecurity, ITU, 2005, hal 11-15. Lihat juga <http://www.conventions.coe.int/treaty/FN/treaties/185.html>, diakses tanggal 25 Oktober, 2010.

43. Convention on Cybercrime 2001.

- Llyod Ian J , 2000, *Information Technology Law*, London : Butterworth.
- Clough Jonathan , 2010, *Principles of Cybercrime*, UK: Cambridge University Press.
- Baylis John & Smith Steve, 2001, *The Globalization of World Politics, An Introduction to International Relations*, New York, Oxford University Press.
- Goesniadhie Kusnu, 2006, *Harmonisasi Hukum dalam Perspektif Perundang-Undangan*, Surabaya : PT. Temprina Media Grafika.
- Sanusi M. Arsyad, 2004, *Teknologi Informasi & Hukum E-commerce*, Jakarta : PT Dian Ariesta , Jakarta.
- Kusumaatmadja Mochtar, Etty R. Agoes, 2003, *Pengantar Hukum Internasional*, Bandung : PT. Alumi.
- Mugasejati Nanang Pamuji dan Ucu Martanto (ed), 2006, *Kritik Globalisasi & Neoliberalisme*, Yogyakarta: Fakultas Ilmu Sosial dan Ilmu Politik UGM.
- Nir Kshetri, 2010, *The Global Cybercrime Industry*, New York : Springer Heidelberg Dordrech.
- Roger LeRoy Miller and Gaylord A. Jentz, 2001, *Law for E-Commerce*, USA : West Thomas Learning.
- Roni Hanitijo Soemitro, 2001, *Metodologi Penelitian Hukum dan Jurimetri*, Jakarta, Ghalia Indonesia.
- Steven Furnel, 2002, *Cybercrime Vandalizing the Information Society*, Great Britain : Pearson Education Limited.
- Soeyono Soekanto, 1982, *Pengantar Penelitian Hukum Edisi Kedua*, Jakarta : UI Press, Jakarta.
- Soeryono Soekanto, 1998, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Jakarta: CV Rajawali.
- Sunaryati Hartono, 2006, *Bhineka Tunggal Ika Sebagai Asas Hukum bagi Pembangunan Hukum Nasional*, Jakarta: Penerbit PT Citra Aditya Bakti .
- Thomas L. Friedman, 2006, *The World is Flat*, London: Penguin Books.
- Branscomb, 1983 , *Information is the Lifeblood that sustain political, social and business decision*, dalam Anne W. Branscomb, *Global Governance of Global Networks: "A survey of Transborder Data Flows in Transition"*, *Vanderbilt Law Review*, Vol. 36.
- Maureen S. Dorney, 1998, "Privacy and the Internet", *Hasting Communications and Entertainment Law Journal*, Vol 19.
- Kofi A. Anan , 2004, dalam *UNCTAD E-commerce and Development Report*.
- Stein Schjolberg, 2010, *A Cyberspace Treaty- A United Nations Convention or Protocol on Cybersecurity and Cybercrime*, Background Paper dalam dalam The Twelfth United Nations Congress on Crime Prevention and Criminal Justice.
- Stein Schjolberg & Amanda M. Hubbard, 2005, *Jenewa, Harmonizing National legal Approaches on Cybercrimw*, Paper dalam WSIS Thematic Meeting on Cybersecurity, ITU, 2005.
- Stein Schjolberg, 2010, Paper dalam Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Brazil.
- Susan W. Brenner and Marc D. Goodman, 2002, *Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice*, Paper.
- Izwan Ismail, 2008, *Understanding Cyber Criminal*, New Straits Times, 18 Februari.
- Petrus Reinhard Golose, 2006, *Perkembangan Cybercrime dan Usaha Penangannya di Indonesia oleh Polri*, Buletin Hukum dan Kebanksentralan, Volume 4 Nomor 2, Agustus .
- Stein Schjolberg, 2010, Paper dalam Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Brazil.
- M o h a m a d S a l a h u d d i e n dalam <http://www.idsirtii.or.id/index.php/news/2010/01/21/81/mewaspadai-kejahatan-layanan-perbankan-elektronik-himbauan-kepada-masyarakat-dan-keterangan-pers.html>, diakses tanggal 10 September, 2010.
- H a m a d o u n T o u r e , <http://www.pwc.com/gx/en/communications/revue/perspective/hamadoun-toure.jhtml>, diakses tanggal 31 Oktober, 2010.
- <http://www.internetworldstats.com/stats.htm>, diakses tanggal 26 oktober, 2010.
- <http://www.oecd.org/dataoecd/53/60/37019786.pdf>, diakses tanggal 10 Desember, 2010.
- <http://www.itu.int/ITU->

D/cyb/cybersecurity/legislation.html, diakses tanggal 10 desember, 2010

<http://www.conventions.coe.int/treaty/commun/cherchsig.html>, diakses tanggal 25 Oktober, 2010.

h t t p : / / www.conventions.coe.int/treaty/EN/treaties/185.html, diakses tanggal 25 Oktober, 2010.

<http://www.justice.gov/> Diakses tanggal 27 Oktober, 2010.

<http://www.smh.com.au/news/technology/nab-closes-eight-bogus-websites-overseas/2005/12/29/1135732681755.html>, diakses tanggal 28 Oktober, 2010.

ITU Toolkit , dalam <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>, halaman

diakses tanggal 25 Oktober, 2010.

Laporan ITU, Understanding Cybecrime for Developing Countries, 2009,dalam <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>, diakses tanggal 24 Oktober, 2010.

<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>, diakses tanggal 24 oktober, 2010.